INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Aug 2023
ISSN: 2582-6433

ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY AND TO CURB CYBER CRIMES IN INDIA

AUTHORED BY - TEJAL MILIND GUJAR
Class: LLM IInd Year, Sem: IIIrd
Roll No.- 16
Progressive Education Society's Modern Law College, Pune

Abstract:

Since we now live in a globally connected internet community, the majority of our daily interactions and business dealings now happen online. Cyberspace is a fast-moving target for threats because cyber infrastructure is extremely prone to them. The safety of cyberspace cannot be achieved just by human interaction or by any physical device due to the enormous volume of data being used and the speed of cyber activity. Making wise decisions in real time and detecting risks require a significant amount of automation. Creating software with traditional techniques to fend off attacks that are constantly changing is challenging. It can be resolved by incorporating artificial intelligence techniques influenced by biology into the program. This study's goal is to investigatethe possibilities of artificial intelligence in addressing the cybercrime issues.[1]

Keywords: Artificial Intelligence, Artificial Neural Network, Artificial Immune System, Intelligent Agents, Genetic Algorithm, Fuzzy, Cyber Crime, Intrusion Detection and Prevention Systems.

Introduction

Since we now live in a globally connected internet community, the majority of our daily interac tions and business dealings now happen online.Concerns concerning the security of information incyberspace are brought up by the expanding trends in internet computing.Cyberspace is open to attacks and unauthorized access.Cyberspace threats travel at the speed of light, aiming at indi

[1] Selma Dilek, Hüseyin Çakır and Mustafa Aydın," Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015

ISSN: 2582-6433

viduals, organizations, and governmental bodies.It goes without saying that only intelligent soft ware can provide defense against intelligent cyberweapons.Owing to the rapid pace of cyber act ivity and the vast amount of data involved, neither physical equipment nor human interaction ca n effectively defend against cyberspacethreats.Making wise decisions in real time and detecting risks require a significant amount of automation.Software development is challenging when usi ng with conventional algorithms to effectively protect against the dynamically evolving attacks. This is why we need innovative approaches such as applying methods of Artificial Intelligence (AI) that provide flexibility and learning capability to software which will assist humans in fighting cybercrimes.[2]

Cyber Crimes

The proliferation of cybercrimes coincides with the expansion of the Internet. Internet crime is perpetrated in a variety of ways and has numerous guises. Cybercrime is the term used to describe unlawful acts carried out via computers and the internet. Cybercrimes stem from the diversity and evolution of the internet worldwide.There are essentially two main types of cybercrime. One of those views network intrusions, system destruction, and other related actions as criminal offenses. The others are the ones who use the network to do illegal activities like fraud.[3]

Even though the term "cybercrime" is now widely used, its exact definition is unclear. "Cybercrime is a term used widely to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity," according to Somaiya et al. (2014).[4]"Offenses that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the Internet and mobile phones," according to Halder et al. (2011), are defined as cybercrimes.[5]. "Cybercrime includes all unauthorized access of information and break security like privacy, password, etc. with the use of the internet," according to Kandpal et al. (2013). Cybercrimes encompass a

[2] Selma Dilek, Hüseyin Çakır and Mustafa Aydın, ”Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015
[3] Manveer Kaur, Sheveta Vashisht, Kumar Saurabhi, “Adaptive Algorithm for Cyber Crime Detection”, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3 (3), 4381 – 4384, 2012
[4] Jheel Somaiya, Dhaval Sanghavi, Chetashri Bhadane, ”A Survey: Web based Cyber Crimes and Prevention Techniques”, International Journal of Computer Applications (0975 – 8887), Volume 105, November 2014
[5] Halder, D. Jaishankar, K, ”Cyber crime and the Victimization of Women: Laws, Rights, and Regulations”. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

ISSN: 2582-6433

broader range of illicit activities involving computers, such as financial crimes, virus attacks, illicit article sales, pornography, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer systems, theft of electronically stored information, e-mail bombing, physical damage to computer systems, and so forth.[6] The statistics that have been obtained and reported about demonstrate the seriousness of Internet crimes in the world. "Phishing" emails alone produce one billion dollars for their perpetrators. In an FBI survey in early 2004, 90 percent of the 500 companies surveyed reported a security breach and 80 percent of those suffered a financial loss. A national statistic in 2003 stated that four billion dollars in credit card fraud are lost each year. Only two percent of credit card transactions take place over the Internet but fifty percent of the four billion, mentioned before, are from the transaction online. All these finding are just an illustration of the misuse of the Internet and a reason why Internet crime has to be slowed down.[7]

Artificial Intelligence

AI (formerly known as machine intelligence) first appeared as a field of study at Dartmouth College's Summer Research Project in July 1956. It is described as "the science and engineering of making intelligent machines" by the term's originator, John McCarthy. "Artificial intelligence is the study of how to make computers do things which, at the moment, people do better," is the widely recognized definition of artificial intelligence. Reasoning, knowledge, planning, learning, natural language processing (communication), perception, and the capacity to move and manipulate objects are among the main issues (or objectives) of AI research. Three things are required of an AI system.

i. Store information
ii. Use that information to solve issues
iii. iii.Gain new information via experience The three main parts of AI are representation, reasoning, and learning[8]

The general problem of simulating intelligence has been simplified to specific sub-problems which have certain characteristics or capabilities that an intelligent system should exhibit. The

[6] Vineet Kandpal and R. K. Singh, "Latest Face of Cybercrime and Its Prevention In India", International Journal of Basic and Applied Sciences, Vol. 2, Pp. 150- 156, 2013
[7] Advocate,VivekTripathi,"InternetCrime",www.cyberlawsindia.net,Available:http://www.cyberlawsindia.net/internet-crime.html
[8] T N Shankar, Neural Networks, LAXMI Publications Pvt.Ltd, 2008

ISSN: 2582-6433

following characteristics have received the most attention: [9]

a. Deduction, reasoning, problem solving
b. Knowledge representation
c. Planning
d. Machine learning
e. Natural Language Processing
f. Motion and Manipulation
g. Perception
h. Social Intelligence
i. Creativity
j. General Intelligence [10]

Conventional AI techniques primarily concentrate on knowledge representation, inference processes, and individual human behavior. Distributed artificial intelligence (DAI), on the other hand, is primarily concerned with social behavior. DAI systems are characterized as cooperative systems in which a group of agents collaborate to find a solution to a specific issue. These agents are frequently diverse. "An agent can be a physical or virtual entity that can act, perceive its environment (in part), communicate with others, is autonomous, and has skills to achieve its goals and tendencies," according to Jacques Ferber (1999). Agents are discrete entities with defined boundaries and problem-solving interfaces. In contrast, a multi-agent system is a loosely coupled network of agents that solves problems together as a single entity, much like a society.[11]

The main applications of multi-agent systems are

- Problem Solving
- Building Synthetic Worlds;
- Multi-Agent Simulation;
- Collective Robotics
- Designing Kenetic Programs

[9] J. S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, Upper Saddle River, Prentice Hall, New Jersey, USA, 2003
[10] G. Luger, W. Stubblefield, Artificial Intelligence: Structures and Strategies for Complex Problem Solving, Addison Wesley, 2004
[11] Jacques Ferber, Multi-Agent System: An Introduction to Distributed Artificial Intelligence, Harlow: Addison Wesley Longman, 1999

ISSN: 2582-6433

Within the field of artificial intelligence, computational intelligence (CI) focuses primarily on heuristic algorithms like fuzzy systems, neural networks, and evolutionary computation. Computational intelligence and "soft computing" are synonymous terms. More recently, the scope of Computational Intelligence techniques has expanded to include new fields like artificial immune systems, swarm intelligence, chaotic systems, etc. Neural networks, fuzzy logic, evolutionary computation, swarm intelligence, machine learning, and artificial immune systems are examples of nature-inspired techniques that offer flexible decision-making mechanisms for problems like cyber security issues.[12]

Yet another AI technique is genetic algorithms.Even for the most complicated computing issues , they offer reliable, flexible, and ideal solutions.They can be applied to intrusion detection syst ems (IDS) to create rules for classification security attacks and to create customized rules for va rious types of security attacks.[13]

Intrusion Detection and Prevention System Intrusion Detection System

(IDS) can provide defense against both internal and external attackers by preventing any traffic from passing through the firewall. A firewall protects a company from malicious Internet and intrusion detection system (IDS) attacks. If an intruder manages to get past the firewall's security measures, they can then attempt to access any trusted system. If there is a security breach, it notifies the system administrator. Similar to a smoke detector, an IDS sounds an alarm when certain conditions are met.

An intrusion detection system, or IDS, is a software or hardware that keeps an eye on system or network activity for any indications of malicious activity or policy violations, then sends reports to a management station. IDS can take two forms: host-based IDS and network-based IDS (HIDS and NDS, respectively).[14]

[12] UKCI, "Workshop on Computational Intelligence", ukci.cs.manchester.ac.uk, Avaliable: http://ukci.cs.manchester.ac.uk/intro.html
[13] N. A. Alrajeh and J. Lloret," Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, Vol.2013, Article ID 351047.
[14] https://en.wikipedia.org/wiki/Intrusion_detection_system

ISSN: 2582-6433

IDS carries out several tasks, including:

- Auditing system configuration for vulnerabilities and misconfigurations; keeping an eye on users and system activity
- Evaluating vital system and data file integrity
- Identifying established attack patterns in system operations
- Utilizing statistical analysis to pinpoint anomalous activity
- Overseeing audit trials and drawing attention to policy or regular activity violations by users
- Setting up and using traps to gather data about trespassers
- Fixing configuration errors in the system A hardware or software system installed inside a network that can both identify potential intrusions and make an effort to stop them is known as an intrusion detection and prevention system, or IDPS.

When compared to conventional techniques, Artificial Neural Networks (ANNs) can improve Intrusion Detection Systems' (IDS) performance. A first step toward creating artificial intelligence is the development of artificial neural networks. ANNs are an information processing system that draw inspiration from the nervous system of a living thing. ANN offers resources that let us create AI.[15]

Applications of AI Techniques in Defending Cyber Crimes

Academic resources that are currently available demonstrate the wide range of uses for AI techniques in the detection and prevention of cybercrime. Neural networks, for example, can be used to create extremely effective intrusion detection and prevention systems. A suggestion to use artificial Neural networks are also used in malware classification, forensic investigation, Denial of Service (DoS) attack detection, computer worm, spam, and zombie detection. In order to increase their effectiveness, newer antivirus systems are utilizing AI techniques like data mining, neural networks, and heuristics. Intelligent agents and mobile agents are sometimes used in distributed wireless intrusion detection systems (IDS). IDS based on mobile agents add mobility features to the network's security by monitoring suspicious cyber activity through mobile agent mechanisms.

[15] Gang Wang, Jinxing Hao, Jian Ma, and Lihua Huang, ”A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering”, Elsevier Ltd 2010

ISSN: 2582-6433

Application of Artificial neural networks against cyber crimes

Comprising of basic processing units, the Artificial Neural Network is a massively parallel distributed processor with an innate ability to store and retrieve experimental knowledge. In 2008, Chen described NeuroNet, a neural network system that can monitor traffic, identify anomalies in it, and then initiate corrective action. The results of the NS-2 experiment demonstrated that NeuroNet is effective against low-rate TC Ptargeted distributed DoS attacks, also referred to as shrew attacks, a particular kind of covert attack.[16]

Machine Learning In Cyber Threat Detection

To stop whatever the enemy is trying to accomplish, organizations need to be able to recognize a cyberattack before it happens. Artificial intelligence's machine learning component has shown to be very helpful in identifying cyberthreats by analyzing data and spotting them before they take advantage of a weakness in your information systems. Artificial intelligence techniques can help overcome various shortcomings of today's cyber security tools because of their flexible and adaptable system behavior. Even though AI has already greatly improved cyber security, there are still valid worries. Some believe that AI poses an increasing existential risk to humanity.

Importance of Cyber Security

To stop whatever the enemy is trying to accomplish, organizations need to be able to recognize a cyberattack before it happens. Artificial intelligence's machine learning component has shown to be very helpful in identifying cyberthreats by analyzing data and spotting them before they take advantage of a weakness in your information systems. Artificial intelligence techniques can help overcome various shortcomings of today's cyber security tools because of their flexible and adaptable system behavior. Even though AI has already greatly improved cyber security, there are still valid worries. Some believe that AI poses an increasing existential risk to humanity. systems are growing. The volume and sophistication of cyberattackers' methods increase as they employ multiple attack techniques, leading to an increase in problems.

[16] E. Tyugu, ”Artificial intelligence in cyber defense”, In Proceedings of the 3rd International Congress on Cyber Conflict (ICCC), pp. 1–11,2011.

ISSN: 2582-6433

Role and Need of AI in Cyber Security

When we talk about artificial intelligence in cyber security, it is nothing new. Because data is at the core of current cyber security trends, two years ago, people used to debate in forums how AI and ML would impact the field of cybersecurity.

Artificial intelligence is useful in cyber security because it helps security professionals better analyze, research, and comprehend cybercrime. It enhances the tools used by businesses to thwart cybercriminals and supports enterprises in protecting consumer information.

On the other hand, artificial intelligence may not be useful in almost every situation and can be a very comprehensive resource. Most significantly, it can also be a new tool for cybercriminals, who can use it to advance their tactics and quicken their pace cyberattacks.

Need for AI in Cyber Security

A typical human being cannot recognize and stop every threat that a company faces since hackers always come up with new ways to launch diverse attack types for varying objectives. For instance, log4j was present from the start but was not well-known until it was reintroduced in December 2021.

If you don't locate, recognize, and take action against these new, unidentified threats, they have the potential to seriously harm the network and the organization.[17]

Benefits of Using Artificial Intelligence in Cybersecurity

AI learns more over time

As the name implies, artificial intelligence technology is more intelligent and efficient because it can gradually strengthen network security. Machine Learning and Deep Learning are utilized by Artificial Intelligence to gain further insights into an organization's network behavior over time. They are able to identify the network's patterns. AI technology recognizes them, groups them together, and then determines if there was a deviation from the usual flow of traffic or a safety incident. When the traffic is finally analyzed, it responds to them.

[17] Ankur Modi & Arunabh Chattopadhyay, Threat Intelligence in India: An Overview, 18 Int'l J. Comp. Applications 14 (2018).

ISSN: 2582-6433

AI identifies unknown threats

Because hackers always come up with new ways to break systems, engineering forces us to move to more contemporary solutions in order to stop new attacks from causing harm. One of the best combinations for security technologies to identify unknown threats and stop them from destroying an organization's network infrastructure is the artificial intelligence that is built into cyber security.

AI is capable of handling a lot of data

Artificial intelligence is the best option because it is very helpful in detecting potential threats that are hidden under seemingly normal activities. Because it is automated, it can scan through massive volumes of data and analyze the traffic to look for any potential threats. Residential Proxy is a technology that facilitates data transfer by utilizing artificial intelligence. In addition, it has the ability to recognize and detect any dangers in the flow of traffic.

Better Overall Security

Because AI protects at both the macro and micro levels, malware has a very difficult time infiltrating corporate networks. By doing this, the overall security posture is improved and IT teams are freed up to handle more sophisticated threats.

Reduce Duplicate Processes

As you are aware, hackers are constantly evolving their tactics. But fundamental security best practices remain constant throughout time. If you employ someone to do this, they might grow disinterested in it and eventually begin to overlook crucial security features, leaving their network vulnerable.

Security Certification

As you are aware, hackers are constantly evolving their tactics. But fundamental security best practices remain constant throughout time. If you employ someone to do this work, they might grow disinterested in it and eventually start overlooking crucial security features, leaving their network vulnerable.

ISSN: 2582-6433

AI Accelerates Detection And Response Times

Threat detection should be the first step in protecting your company's network. If you could identify distorted data instantly, that would be ideal. In addition to saving you time, this will prevent irreversible network damage. By combining AI with cyber protection, you can quickly scan the entire system to look for any potential threats.

How does AI in cybersecurity help to avoid cyberattacks?

Cybersecurity benefits from artificial intelligence on both a global and micro level. When seen from a wider angle, Next Generation Firewalls (NGFW) provide excellent protection for an organization. When comparing the current cyber threats, embedded machine learning algorithms detect and quarantine suspicious files without utilizing any kind of prior signature-based database.

ML algorithms are used to identify particular behaviors in a file. If a file surpasses a predetermined threshold, it is isolated and subjected to analysis.

If a file satisfies specific thresholds after the ML algorithm identifies it as exhibiting particular characteristics, it is isolated and examined further. With every use of the ML algorithm, NGFW Firewall gets better at identifying suspicious files by taking lessons from the behavior that has already been tested.

Since NGFW firewalls do not use any offline technology that reduces network performance, users do not notice any decrease in network response time.

Heuristic analysis-based detection techniques are used by anti-malware software from a subtle, device-level perspective. To put it another way, AI finds possible infections that have never been identified before.

Virus software operates in a different way. Antivirus software uses a technique called signature-based detection, which compares the signature of a known virus to one that has already been identified and stored in a signature database. Antivirus software won't be able to stop the online

ISSN: 2582-6433

threat if it hasn't been exposed to this infection.[18]

How Does AI Solve Cybersecurity Challenges?

As we've already discussed, the best defense against cyberattacks for your business is to fight fire with fire. And in this instance, it's because hackers are using AI to implement sophisticated hacking techniques. AI can be used to identify vulnerabilities or weaknesses in the same way that it uses data to identify threats.

Some criminals might even turn the AI model backwards in order to access private information and effectively take over a company's cybersecurity. AI is also utilized in other contexts to scale up massive operations that mine networks, devices, and applications for vulnerabilities. AI can improve almost every tactic employed by cybercriminals.

Future of Artificial Intelligence in Cyber Security

- AI has a bright future in cybersecurity, no question about it. For the following reasons:
- Threats can be recognized faster and more precisely than by people.
- Prevent attacks by automatically blocking suspicious activity.
- Strengthen network defenses against attacks.
- Accelerate the process of cyberattack recovery.
- Strengthen digital systems' overall security.
- AI is already starting to help cybersecurity. It will become increasingly more important in the future. To stay ahead of the curve, businesses should start investing in AI-based security solutions immediately.

India's capacity to combat cybercrimes and the necessity of doing so:
The issue of cybercrime is on the rise in India, as it is in numerous other countries worldwide. The increased use of technology and the internet has increased the risk of cyberattacks and other cybercrimes. Major societal and economic repercussions from these crimes may include lost personal information, financial losses, and harm to one's reputation.

[18] S. Dilek, Hakır and M. Aydın,"Applications Of Artificial Intelligence Techniques To Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications (IJAIA), vol. 6, no. 1, 2015.

ISSN: 2582-6433

India has witnessed several high-profile cases of ransomware attacks, phishing scams, data breaches, and online fraud in the past few years. In addition to people and businesses, these crimes affect vital infrastructure and national security.

- One strategy to lessen cybercrime could be to use artificial intelligence (AI). AI can help detect and thwart cyberattacks before they occur, as well as recognize and react to threats more quickly and effectively.AI can also be utilized to automate cybersecurity-related tasks like threat detection and response. As a result, security teams may be more productive because they can focus on more challenging issues. AI may also be utilized to develop more secure systems and identify vulnerabilities before thieves can exploit them.
- The government unveiled the National Cyber Security Policy in 2013, outlining the country's strategy for protecting its cyberspace. Establishing a workforce with the necessary abilities to fight cybercrimes, creating a safe and resilient cyberspace, and promoting cybersecurity innovation are the objectives of the policy.

As a result, India must address cybercrimes immediately. These offenses have the potential to cause significant harm to individuals, companies, and the country as a whole. Artificial intelligence (AI) has a great deal of promise to lower these crimes, strengthen cybersecurity defenses, and thwart cyberattacks.[19]

Current Status of Cybercrime in India:

1. In recent years, cybercrimes have sharply increased in India, according to the National Crime Records Bureau (NCRB). The latest report on crime data in India by the NCRB shows that there were 44,546 recorded cases of cybercrime in 2019. This represents a 63.5% rise over the previous year.

2. Cybercrime Types in India:

- Financial frauds include credit/debit card fraud, online banking fraud, and phishing schemes.
- Hacking: Hacking is the act of gaining unauthorized access to a network or computer system.

[19]Muhammad Adnan Hashmi, Abubakr Muhammad, and Syed Muhammad Ali Abbas, "Artificial Intelligence Techniques for Cybersecurity: An Overview of Use Cases," IEEE Access, vol. 8, 2020, pp. 192267-192281.

ISSN: 2582-6433

- Cyberstalking and harassment: These include bullying, harassment, and stalking that takes place on the internet or on social media.
- Identity theft: Theft of a person's name, address, social security number, and other personal information is known as identity theft.
- Theft of intellectual property: This refers to the stealing of rights pertaining to things like copyrights, trademarks, and patents.

1. **The effects of cybercrime**

- Monetary loss:
  Cybercrimes can result in significant financial losses for both individuals and businesses since hackers usually target financial information.

- Reputational damage:
  Cybercrimes have the power to permanently damage a person's or an organization's reputation.

- Loss of information:
  Cybercriminals have the ability to steal private information, such as financial or personal data, which can lead to identity theft and fraud.

- Legal consequences:
  Cybercrimes are against the law, and those found guilty may face legal consequences.
  In India, cybercrimes pose a significant risk to individuals and enterprises alike, so it's critical to take the appropriate safety measures to guard against them. It's crucial to use strong passwords, keep your software up to date, and refrain from clicking on dubious emails and websites. It's also crucial to report any cybercrimes to law enforcement right away:

Methods Used to Curb Cybercrimes in India:

Some common tactics used in India to combat cybercrime are the Cybercrime Cells, the National Cyber Security Policy of 2013, and the IT Act of 2000.

ISSN: 2582-6433

Some of the methods to curb cyber crimes in India are as following:

- Every Indian state has established Cyber Crime Cells, specialized units, to combat cybercrimes. Investigating and prosecuting cybercrimes is the responsibility of these cells in conjunction with the local police department. The Cyber Crime Cells are equipped with the most recent technology and tools to investigate cybercrimes, and they are staffed by qualified individuals who are experts in cybercrime investigation.
- The IT Act of 2000 was created to create a legal framework for e-commerce and to grant legal validity to electronic transactions. Cybercrimes including hacking, identity theft, phishing, and cyber stalking are covered by the Act's provisions. In addition to sanctions and punishment for cybercrimes, the Act provides provisions for the establishment of Cyber Appellate Tribunals to hear appeals against the rulings of Adjudicating Officers.
- The National Cyber Security Policy of 2013 was unveiled to provide a framework for the defense of India's cyberspace. The policy aims to create a secure cyber ecosystem and improve the cyberspace regulatory framework. The strategy also intends to establish partnerships with industry, academia, and other relevant parties in order to disseminate cybersecurity knowledge and develop innovative cybersecurity solutions.
- In addition to these traditional methods, the Indian government has established the Indian Computer Emergency Response Team (CERT-In) to quickly respond to cyberattacks and coordinate responses with other government agencies, business partners, and international organizations.[20]

Overall, these traditional methods have been successful in lowering cybercrimes in India; however, ongoing investments in cybersecurity infrastructure and training for law enforcement organizations such as; are still necessary to keep up with the ever-evolving nature of cyber threats:

The 2000 IT Act:

The IT Act of 2000 was created to provide electronic transactions with legal standing and to create a framework for e-commerce. The Act's provisions apply to cybercrimes such as hacking, identity theft, phishing, and cyberstalking. In addition to sanctions and punishment for cybercrimes, the Act provides provisions for the establishment of Cyber Appellate Tribunals to hear appeals against the rulings of Adjudicating Officers.

[20] S. Singh and S. Silakari, "A Survey of Cyber Attack Detection Systems", IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 5, 2009.

ISSN: 2582-6433

According to Section 43 of the IT Act, gaining unauthorized access to a computer system, computer network, or computer resource is illegal. Section 66 criminalizes hacking, and Section 66A criminalizes sending offensive communications through communication services. Phishing is covered in Part 66C and identity theft in Section 66B.

The 2013 National Cyber Security Strategy:

In order to create a comprehensive plan for safeguarding India's online territory, the National Cyber Security Policy was introduced in 2013. The policy aims to create a secure cyber ecosystem and improve the cyberspace regulatory framework. The strategy also intends to establish partnerships with industry, academia, and other relevant parties in order to disseminate cybersecurity knowledge and develop innovative cybersecurity solutions.

In conclusion, traditional measures like the Indian Computer Emergency Response Team (CERT-In), the IT Act of 2000, the National Cyber Security Strategy of 2013, and Cyber Crime Cells have all helped India successfully reduce the amount of cybercrimes. Nonetheless, law enforcement organizations need to keep funding cybersecurity infrastructure and training in order to keep up with the evolving nature of cybercrime.

Efficient Use of Artificial Intelligence Approaches to Reduce Cybercrimes

It includes a variety of tactics to guard against tampering, unauthorized use, and hacker attacks while maintaining the integrity of programs, networks, and stored data. Proper implementation of cyber security prevents identity theft, data breaches, and other cyberattacks by hackers. Cybersecurity thus makes it possible to secure data against unauthorized access, alteration, and destruction.

The following are some ways AI could lower India's cybercrimes:

Monitoring for cybersecurity:

Artificial intelligence (AI) can be used to monitor network activity and identify any anomalies that might indicate a cyberattack. Artificial intelligence (AI) systems have the capacity to identify threats instantly, identify patterns in network traffic, and alert security personnel before a breach occurs.

- **Fraud detection:**

  Credit card fraud and money laundering are two examples of financial transaction fraud

ISSN: 2582-6433

that artificial intelligence (AI) systems can be trained to detect. AI can use data trends to identify suspicious activity and alert authorities.

- **Malware detection:**
  Artificial intelligence (AI) can locate and remove malware by looking at code and behavior patterns. Through the analysis of code structure and behavior, artificial intelligence (AI) can identify novel malware types and prevent them from compromising computers.

- **Predictive analysis:**
  AI is able to identify potential cyber threats ahead of time through predictive data analysis. AI uses machine learning algorithms to identify patterns in data, which enables security teams to take proactive measures by anticipating potential threats.

- **Support for investigations:**
  AI is able to analyze large volumes of data and identify patterns that may indicate the source of an attack, which can be helpful in cybercrime investigations. Identifying suspects and building a case against them can both benefit from this.

  AI has the power to drastically lower cybercrimes in India. Capability to analyze large volumes of data, identify anomalies, and identify potential threats could significantly strengthen the country's cybersecurity posture.

In order to identify and prevent crime in India, some AI tools that can be employed are as follows:

- **Phishing detection:**
  Phishing is a widespread cybercrime in which criminals deceive victims into divulging critical information by sending emails, using social media, or using messaging apps. By examining the content of emails, links, and attachments, AI-based systems can assist in the detection of phishing assaults. Artificial intelligence (AI) algorithms are able to spot suspicious trends in email content or URL links and flag them for additional examination. AI may also examine the email's origin to determine whether it originates from a known phishing domain.

ISSN: 2582-6433

- **Threat Intelligence:**

  An AI-powered service called threat intelligence gathers and examines data from various sources in order to identify possible security risks. With the help of this technology, businesses can proactively stop attacks and remain updated about emerging security threats. To determine where to focus their cybersecurity efforts, businesses can utilize threat intelligence to spot patterns and trends in cyberattacks.

Security Information and Event Management (SIEM):

Security information and event management, or SIEM, is an AI-based system that integrates security information management and security event management to detect and manage cyber threats. SIEM gathers and examines log data from multiple systems and applications in order to provide alerts in real time when a potential threat is detected. Security personnel can act quickly when patterns in log data point to a cyberattack because SIEM's AI algorithms do so.[21]

Implementing AI-based solutions in India

Lack of Standardization:

The lack of standards for AI-based solutions in India could lead to interoperability issues. Since different vendors use different frameworks, integrating solutions from multiple suppliers can be difficult. Scaling up solutions might be challenging as a result.

Regulatory Framework:

India does not have a comprehensive artificial intelligence regulatory framework. This could lead to concerns about the application and regulation of AI. A clear regulatory framework is necessary to ensure that AI is developed and used in an ethical and responsible manner.

Bias in Data:

One of the main issues with AI is data bias, which exists in India as well. Artificial intelligence-based solutions frequently use skewed data sets that benefit specific populations, like urban areas or specific demographic groups. It can be challenging to eliminate bias from data sets, which could have discriminating effects on AI-based solutions.

[21] Siems.gov.com.in

ISSN: 2582-6433

All things considered, implementing AI-based solutions in India is not without its challenges. If India makes the right investments in human capital, infrastructure, and legal frameworks, it can overcome these challenges and emerge as a global leader in artificial intelligence innovation.[22]

Conclusion

To Conclude, there is great potential for artificial intelligence (AI) to lower cybercrime in India. Given the rise in cybercrimes, it is imperative to take advantage of AI's ability to detect, stop, and react to them swiftly and efficiently. It is possible to identify patterns, anomalies, and other indicators of cyberattacks using deep learning, machine learning, and other AI-based technologies.

Law enforcement organizations can also use AI to track down and apprehend cybercriminals, analyze vast volumes of data to identify unusual activity, and anticipate and thwart future attacks. Through the integration of information into cybersecurity systems, India can stay ahead of the rapidly evolving cyber threat landscape and protect its citizens from the damaging effects of cybercrime.

Due to the high volume of activity on the company network, a typical medium-sized startup or business experiences high traffic. This indicates that a significant amount of data is sent between clients and staff members on a daily basis. In order to prevent hackers from reading or altering the transferred data and causing harm to both the user and the organization, it is imperative that the data be secured against them. It becomes impractical for cyber security professionals to review every communication in order to identify possible risks.

Artificial intelligence is quickly becoming a top innovation for enhancing IT security teams' performance. People interested in cyber security can benefit from technologies' solid grasp of computer networks. Security experts can use AI to limit breach risk and maintain security posture by using the necessary analysis and threat identification evidence. Humans may never be able to scale back to the point where they can adequately secure an enterprise-level attack surface. is possible to enhance.

[22] https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

ISSN: 2582-6433

AI can also help identify and prioritize risks, manage incident response, and isolate hacker attacks before they happen in a scenario. Therefore, even with the anticipated drawbacks, AI will effectively progress cyber security and assist the company in implementing a stronger security posture.